

Presseinformation

29. November 2016

Onlinebanking ohne Trolle

Immer öfter tappen Bankkunden in die E-Mail-Falle. In der Inbox finden Sie eine Nachricht ihrer vermeintlichen Bank mit der Aufforderung, einen Umsatz zu prüfen, oder Kontodaten zu bestätigen. Dazu sollen Sie auf einen Link klicken. Und genau dies sollten Sie niemals tun! Nicht aus Neugier, nicht weil Sie sich unter Druck gesetzt fühlen. Denn der Klick führt sicher dazu, dass Sie sich Schadsoftware (z.B. Trojaner) auf den PC laden, die Ihre geheimen Daten auslesen kann. Die Bank schickt ihren Kunden niemals E-Mails, um sich etwas bestätigen zu lassen und sie schickt Ihnen schon gar keine weiterführenden Links.

Kontakt

Julia Topar
Bundesverband
deutscher Banken
e.V.
Leiterin Finanz-
bildung und Veran-
staltungen, Director
Tel. +49 30 1663
1290

julia.topar@bdb.de

Schlagworte

PIN
TAN
Verbraucher
Onlinebanking
Phishing



Was viele nicht wissen: Der PC zu Hause ist das Einfallstor Nummer eins für Kriminelle. Installieren Sie deshalb einen

Presseinformation

Auch die Software sollte immer auf dem neuesten Stand sein. Sobald Sie ein Update angeboten bekommen, nutzen Sie es und zögern die Installation nicht hinaus. Das gehört zu Ihren Sorgfaltspflichten als Online-Banking-Kunde.

- Speichern Sie niemals Kennwörter, Ihre Geheimzahl (PIN) und TANs in Apps, in der Cloud oder auf Ihrer Festplatte. Auch nicht als Telefonnummern verschlüsselt im Handy.
- Zudem sollte man immer darauf achten, dass die Zugangsdaten nur eingegeben werden, wenn man sich auf der geschützten Seite der Bank befindet und eine verschlüsselte Verbindung besteht. Das lässt sich unter anderem daran erkennen, dass die Internetadresse der Bank mit https:// beginnt.

Während der Onlinebanking-Sitzung sollten Sie niemals:

- mehrere TANs eingeben, auch nicht nach Aufforderung.
- eine TAN zur Aufhebung einer angeblichen Kontosperrung oder zur Laufzeitbeschränkung Ihrer iTAN-Liste eingeben.
- eine Rücküberweisung einer (vermeintlich) eingegangenen Zahlung vornehmen.
- eine Testüberweisung durchführen.
- eine Sicherheitssoftware installieren.

Wenn Sie diese Tipps beherzigen, können Sie Ihr Onlinebanking sicher und bequem nutzen. Sollten Sie tatsächlich Opfer von Phishing-Betrügern werden, wenden Sie sich umgehend an Ihre Bank und lassen Sie das Konto sofort sperren.

Mehr zu PIN, TAN und Signaturverfahren können Sie [hier](#) nachlesen.